UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,601	06/27/2003	Haixiang He	15918ROUS01U	2261

34645 7590 12/05/2006

JOHN C. GORECKI, ESQ.
P.O BOX 553
CARLISLE, MA 01741

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/608,601	HE, HAIXIANG	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 9-18* is/are rejected.

7)☒ Claim(s) *8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/25/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed August 25, 2003 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claim 12 is claiming the control logic in the wireless access point. Control logic, as described in the specification (page 12, lines 20-31) is not limited to one of the four statutory classes on an invention. In the section cited above, applicant discloses "programmable logic can also be fixed in a computer data signal embodied in a carrier wave". Computer signals embodied in a carrier wave do not fall into one of the four statutory classes on an invention.

Claims 13-18 depend from claim 12. None of the dependent claims cure the deficiency of independent claim 12 and therefore each are considered non-statutory for the same reasons given above for claim 12.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7 an 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over US patent application 20020129271 granted to Stanaway, JR. et al. and further in view of US patent 6,976,177 granted to Ahonen.

Regarding claim 1, Stanaway teaches a method for establishing a VPN tunnel with a network by passing identifying information associated with a user to a VPN host network; evaluating the identifying information by the VPN host network to obtain an access result; and granting access to the user on wireless network based on the access result." see paragraph [0018] (. . . The user then begins a process for the establishment of a VPN using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client, password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2. However, Stanaway fails to specifically teach a wireless user connecting to a wireless network. Ahonen teaches a virtual private network system where a mobile

terminal establishes a secure wireless communication with a VPN host via a security gateway (see column 2, lines 25-30). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ahonen's wireless virtual private network implementation with Stanaway's virtual network protocols for the purpose of allowing users the flexibility of mobile computing. One of ordinary skill in the art would have been motivated to provide a wireless VPN in order to meet the increasing demand for mobility in communication systems (see Ahonen; column 1, lines 11-12).

Regarding claim 2, Stanaway as modified teaches the step of evaluating comprises authenticating the wireless user based on the identifying information associated with the wireless user, and ascertaining whether the user is authorized to access at least one of the VPN host network and the wireless network." see Stanaway; paragraph [0018] (. . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.) and Figures 1 and 2.

Regarding claim 3, Stanaway as modified teaches the identifying information comprises a conceptual ID, user ID and password." see Stanaway; paragraph [0018] (. . . The user then begins a process for the establishment of a VPN using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client,

password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2.

Regarding claim 4, Stanaway as modified teaches the step of passing identifying information to the VPN host network comprises receiving by the wireless network the identifying information, and transmitting by the wireless network at least a subset of the identifying information to the VPN host network." see Stanaway; paragraph [0018] (. . . The user then begins a process for the establishment of a VPN using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client, password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2.

Regarding claim 5, Stanaway as modified teaches the identifying information comprises at least a conceptual ID, user ID and password, and wherein the subset of the identifying information comprises the user ID and password." see Stanaway; paragraph [0018] (. . . The user then begins a process for the establishment of a VPN

using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client, password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2. (The conceptual ID is considered the IP address of the gateway in the above section and user ID is considered user name).

Regarding claim 6, Stanaway as modified teaches the conceptual ID is not encrypted when received by the wireless network, and wherein the user ID and password are encrypted when received by the wireless network, and wherein the wireless network does not decrypt the user ID and password prior to transmitting the subset of the identifying information to the VPN host network." see Stanaway; paragraph [0018] (. . . The user then begins a process for the establishment of a VPN using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client, password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then

performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2. (The conceptual ID is considered the IP address of the gateway in the above section and user ID is considered user name).

Regarding claim 7, Stananway as modified teaches a step of establishing a VPN tunnel between the VPN host network and the wireless network." see Ahonen; column 2, lines 25-30.

Regarding claim 9, Stananway as modified teaches assigning, by the VPN host network, an IP address for use by the wireless user." see Stanaway; paragraph [0018] (. . . The user then begins a process for the establishment of a VPN using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client, password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2.

Regarding claim 10, Stananway as modified teaches a step of enabling the wireless user to access an established VPN tunnel with the VPN host network." see Stanaway; paragraph [0018] (. . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . .

is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2.

Regarding claim 11, Stananway as modified teaches a step of establishing an encrypted session between the wireless user and the wireless network, and establishing a VPN tunnel between the wireless network and the VPN host network." see Stanaway; paragraph [0018] (. . . The user then begins a process for the establishment of a VPN using the assigned IP address . . . at the security gateway. . . The first packet transmitted to the security gateway identifies as a non-encrypted destination, the IP address of the gateway and includes internal data . . . The internal data will include . . . user name, e.g. client, password and a security ID . . . The data portion or payload . . . will be encrypted . . . the controller thread decrypts the packet data and identifies the user identity, password and security ID . . . An authentication protocol . . . is then performed to authenticate the user's access . . . if authentication is successful the controller . . . establish and maintain a VPN connection.); paragraph [0019] and Figures 1 and 2.

Allowable Subject Matter

Claim 8 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claim 8, the cited prior art fails to specifically teach the wireless network includes a wireless access point, and wherein the VPN tunnel is established between the VPN host network and the wireless access point.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Weiss et al. (US 2002/0144144) discloses a method for controlling virtual private network devices.

B. Watanabe et al. (US 2004/0192309) discloses a method for establishing a virtual private network in a heterogeneous access networks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew B Smithers
Primary Examiner
Art Unit 2137